IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant(s)	:	Carey W. BUNN	Group Art Unit: 2139
Appln. No.	:	10/743,119	Examiner: Schmidt, Kari L.
Filed	:	December 22, 2003	Confirmation No.: 7503
For	:	METHOD FOR PROVIDING NETWORK PERIMETER SECURITY ASSESSMENT	

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Commissioner for Patents
United States Patent and Trademark Office
Customer Service Window, Mail Stop Appeal Brief-Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This appeal is from the Examiner's rejection of claims 1-20 as set forth in the Final Office Action dated September 18, 2007. A Notice of Appeal was timely submitted with appropriate fee payment on December 18, 2007. Accordingly, this Appeal Brief is being timely submitted by the initial due date of February 19, 2008 (i.e., two months from the filing of the Notice of Appeal, with February 18 falling on a holiday). Payment of the requisite fee under 37 C.F.R. §41.20(b)(2) is submitted herewith.

No additional fee is believed to be required for filing the instant Appeal Brief. However, if for any reason the necessary fee is not associated with this file, the undersigned authorizes the charging of any filing fees for the Appeal Brief and/or any necessary extension of time fees to Deposit Account No. 09-0457.

(I) REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation of Armonk, New York, assignee of the entire interest in the above-identified application by an assignment recorded in the U.S. Patent and Trademark Office on December 22, 2003, at Reel 014841and Frame 0605.

(II) RELATED APPEALS AND INTERFERENCES

The Appellants, their legal representatives and the Assignees are not currently aware of any appeals, interferences, or judicial proceedings that may directly affect or be directly affected by or have some bearing on the Board's decision in this appeal. Attached hereto is a Related Proceedings Appendix showing no related appeals or interferences.

(III) STATUS OF THE CLAIMS

In the Final Office Action dated September 18, 2007, claims 1-20 are pending and rejected. No claims are allowed or canceled. Accordingly, claims 1-20 are being appealed and are listed in the "Claims Appendix" attached herewith.

(IV) STATUS OF THE AMENDMENTS

All amendments to the claims have been entered. Accordingly, claims 1-20 as presented in the amendment filed June 28, 2007, are being appealed and are listed in the "Claims Appendix" attached herewith.

(V) SUMMARY OF THE CLAIMED SUBJECT MATTER

Independent Claim 1

By way of non-limiting example, the invention provides a method for checking network perimeter security. The method comprises reviewing security of a network perimeter architecture (step 230, FIG. 2; page 11, lines 1-4; step 410, FIG. 3; page 12, lines 11-20; FIG. 6). The method also includes reviewing security of data processing devices that transfer data across the perimeter of the network (step 240, FIG. 2; page 11, lines 4-7; step 430, FIG. 4; page 13, lines 1-12; FIG. 7).

Additionally, the method includes reviewing security of applications that transfer data across said perimeter (step 260, FIG. 2; page 11, lines 11-13; step 450, FIG. 4; line 13 of page 13 through line 4 of page 14; FIG. 9). The method further comprises reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (step 250, FIG. 2; page 11, lines 7-11; step 470, FIG. 4; page 14, lines 5-16; FIG. 8). The method also includes generating a report concerning security of said perimeter based upon all of the reviewing steps (step 270, FIG. 2; page 11, lines 13-15)

Independent Claim 16

By way of non-limiting example, the invention provides a computer program product comprising a computer usable medium having a computer readable program embodied in the medium (FIG. 3; line 16 of page 11 through line 6 of page 12). The computer readable program, when executed on a computing device, is operable to cause the computing device to review security of a network perimeter architecture (step 230, FIG. 2; page 11, lines 1-4; step 410, FIG. 3; page 12, lines 11-20; FIG. 6).

The computer readable program also causes the computing device to review security of data processing devices that transfer data across the perimeter of the network (step 240, FIG. 2; page 11, lines 4-7; step 430, FIG. 4; page 13, lines 1-12; FIG. 7). The computer readable program also causes the computing device to review security of applications that transfer data across said perimeter (step 250, FIG. 2; page 11, lines 7-11; step 470, FIG. 4; page 14, lines 5-16; FIG. 8).

The computer readable program also causes the computing device to review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (step 250, FIG. 2; page 11, lines 7-11; step 470, FIG. 4; page 14, lines 5-16; FIG. 8). The computer readable program also causes the computing device to generate a report concerning security of said perimeter based upon all said reviews (step 270, FIG. 2; page 11, lines 13-15)

Independent Claim 18

By way of non-limiting example, the invention provides a system comprising a network 154 having a perimeter and a terminal 140 connected to the network 154 (FIG. 1; line 5 of page 9 through line 16 of page 10). The terminal 140 is arranged to review security of a network perimeter architecture (step 230, FIG. 2; page 11, lines 1-4; step 410, FIG. 3; page 12, lines 11-20; FIG. 6).

The terminal 140 is also arranged to review security of data processing devices that transfer data across the perimeter of the network (step 240, FIG. 2; page 11, lines 4-7; step 430, FIG. 4; page 13, lines 1-12; FIG. 7). The terminal 140 is also arranged to review security of applications that transfer data across said perimeter (step 250, FIG. 2; page 11, lines 7-11; step 470, FIG. 4; page 14, lines 5-16; FIG. 8).

The terminal 140 is also arranged to review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (step 250, FIG. 2; page 11, lines 7-11; step 470, FIG. 4; page 14, lines 5-16; FIG. 8). The terminal 140 is also arranged to generate a report concerning security of said perimeter based upon all said reviews (step 270, FIG. 2; page 11, lines 13-15).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-20 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Pat. Pub. No. 2003/0028803 issued to Bunker, V. et al. ("Bunker").

(VII) ARGUMENTS

Claims 1-20 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Pat. Pub. No. 2003/0028803 issued to Bunker, V. et al. ("Bunker").

Claims 1-15

Independent Claim 1 and Dependent Claims 3-5 and 7-11

The rejection of independent claim 1 and dependent claims 3-5 and 7-11 under 35 U.S.C. §102(b) is in error, and the decision to reject these claims should be reversed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP §2131. Appellants submit that the applied art does not show each and every feature of the claimed invention.

Appellants' invention relates in general to network security, and more particularly to a method for providing network perimeter security assessment. As opposed to prior art systems in which any given security tool is specific to a single discipline, embodiments of the invention provide a comprehensive network perimeter security assessment. By providing a method for checking network perimeter security that incorporates more than one network security discipline, an enterprise architecture that is more secure from attacks to computers and network devices may be developed. More specifically, independent claim 1 recites plural (e.g., four) reviewing steps and generating a report concerning security of the perimeter based upon all of the reviewing steps. Particularly, independent claim 1 recites:

> ...reviewing security of a network perimeter architecture;
> reviewing security of data processing devices that transfer data across the perimeter of the network;
> reviewing security of applications that transfer data across said perimeter;
> reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and
> generating a report concerning security of said perimeter based upon all of the reviewing steps.

The Examiner asserts that Bunker discloses all of the features of independent claim 1 at paragraphs 0010 and 0012 (Final Office Action, pages 2-3). Appellants respectfully disagree, and submit that Bunker does not disclose (i) reviewing security of a network perimeter architecture, (ii) reviewing security of data processing devices that transfer data across the perimeter of the network, or (iii) reviewing security of applications that transfer data across said perimeter. Moreover, as Bunker does not disclose these reviewing steps, Appellants submit that Bunker cannot reasonably be said to disclose generating a report based upon all of the recited reviewing steps (e.g., a network perimeter architecture review; a device review; an applications

review; and a vulnerability of devices and applications review), as recited in the claimed invention.

As indicated in Bunker's title, and at numerous instances throughout the specification, Bunker discloses a network vulnerability assessment system and method. That is, Bunker discloses a methodology for determining the vulnerability of a customer system by launching numerous basic tests that simulate hackers attempting to harm the customer system. This is demonstrated by the following passages of Bunker:

> [0010] ... The preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. External vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk level without affecting customer operations. This assessment may be performed over the Internet for domestic and worldwide corporations.
>
> ...
>
> [0069] Figuratively, the Command Engine 116 is the "brain" that orchestrates all of the "basic tests" 516 into the security vulnerability attack simulation used to test the security of customer systems and networks 1002. While the Command Engine 116 essentially mimics hackers, the tests 516 themselves should be harmless to the customer. Each basic test 516 may be a minute piece of the entire test that can be launched independently of any other basic test 516. The attack simulation may be conducted in waves, with each wave of basic tests 516 gathering increasingly fine-grained information.
>
> ...
>
> [0094] The Testers 502 house the arsenals of tools 514 that can conduct hundreds of thousands of hacker and security tests 516. The Tester 502 may receive encrypted basic test instructions from the Gateway 118, via the Internet. The instructions inform the Tester 502 which test 516 to run, how to run it, what to collect from the customer system, etc. Every basic test 516 may be an autonomous entity that may be responsible for only one piece of the entire test that may be conducted by multiple Testers 502 in multiple waves from multiple locations. Each Tester 502 can have many basic tests 516 in operation simultaneously. The information collected by each test 516 about the customer systems 1002 may be sent to the Gateway 118.

As such, Bunker discloses performing a multi-wave vulnerability test. More specifically, Bunker discloses a "Network Vulnerability Assessment System and Method" in which multiple testers 502 attack a network using known hacker tools to assess the vulnerability of the network. However, Bunker is only describing a vulnerability test. Contrary to the claimed invention, Bunker does not disclose: (i) reviewing security of a network perimeter architecture; (ii) reviewing security of data processing devices that transfer data across the perimeter of the network; or (iii) reviewing security of applications that transfer data across said perimeter, as recited in the claimed invention. Instead, Bunker only discloses vulnerability testing. Bunker does not disclose the other three types of security reviews recited in the claimed invention.

The paragraphs of Bunker cited by the Examiner (i.e., paragraphs 0010 and 0012) do not disclose the other reviewing steps as recited in claim 1 and as set forth in Appellants' specification. Instead, these paragraphs of Bunker simply state:

> [0010] To answer the security needs of the market, a preferred embodiment was developed. The preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. External vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk level without affecting customer operations. This assessment may be performed over the Internet for domestic and worldwide corporations.
> ...
> [0012] The preferred embodiment includes a Test Center and one or more Testers. The functionality of the Test Center may be divided into several subsystem components, possibly including a Database, a Command Engine, a Gateway, a Report Generator, an Early Warning Generator, and a Repository Master Copy Tester.

Appellants submit that the description provided in these paragraphs does not explicitly or impliedly disclose *reviewing security of a network perimeter architecture*, as recited in claim 1 and as defined in Appellants' specification. Moreover, these paragraphs do not disclose *reviewing security of data processing devices that transfer data across the perimeter of the*

network, as recited in claim 1 and as defined in Appellants' specification. Furthermore, these paragraphs do not disclose *reviewing security of applications that transfer data across said perimeter*, as recited in claim 1 and as defined in Appellants' specification. Instead, these paragraphs only disclose reviewing the vulnerability of a network (paragraph 0010) and performing the vulnerability review using a Test Center whose functionality may be divided into several subsystem components (paragraph 0012). However, a vulnerability review is only one of four reviewing steps recited in claim 1; and Bunker fails to disclose the other three recited reviewing steps.

Moreover, because Bunker does not disclose all of the reviewing steps recited in claim 1, it is arguably impossible for Bunker to disclose generating a report concerning security of said perimeter based upon all of the reviewing steps, as further recited in claim 1. Therefore, Bunker fails to disclose each and every feature of claim 1, and does not anticipate the claimed invention.

Appellants note that, in box 11 of the Advisory Action dated December 12, 2007, the Examiner refers to "Irvin" as disclosing certain features of claim 1. Appellants submit that if the Examiner is relying on a second reference (i.e., Irvin) to show features that are absent from Bunker, this renders the rejection of claim 1 unsustainable, since "a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). [emphasis added]. See MPEP §2131.

For all of the above-noted reasons, Appellants submit that Bunker does not anticipate independent claim 1. Moreover, as claims 3-5 and 7-11 depend from independent claim 1, these claims, too, are distinguishable from the applied art. Accordingly, Appellants respectfully

request that the Board reverse the rejection of claims 1, 3-5, and 7-11 and return the application to the examining group for allowance.

Claim 2

The rejection of claim 2 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 2 depends from allowable independent claim 1, and additionally recites *reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter.* The Examiner contends that Bunker discloses these features at paragraphs 0122 and 0125 (Final Office Action, pages 3-4). Appellants respectfully disagree.

The passages identified by the Examiner describe how a tester 502 of Bunker's system is placed external to the network 1002 before the vulnerability testing begins. Paragraph 0122 describes how the tester 502 is physically configured for remote administration. Paragraph 0125 describes how the test center 102 verifies the identity of the tester 502 before vulnerability testing actually begins. However, these passages do not disclose *reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter.* There is no mention in these passages of reviewing a data processing device within the perimeter, much less of reviewing a data processing device within the perimeter that authenticates computers or users outside of said perimeter. Instead, in these passages, Bunker is merely describing establishing and identifying the integrity of remote testers 502 before vulnerability testing even begins.

Accordingly, Appellants respectfully request that the rejection of claim 2 be reversed, and the application returned to the examining group for allowance.

Claim 6

The rejection of claim 6 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 6 depends from allowable independent claim 1, and additionally recites *each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network.* The Examiner contends that Bunker discloses these features at paragraphs 0059, 0149, 0054, and 0019 (Final Office Action, pages 8-10). Appellants respectfully disagree.

None of the passages identified by the Examiner disclose a security policy of an enterprise which owns or controls said network, much less that each of the reviews is performed by comparison to such a security policy. Instead, paragraph 0059 describes performance metrics for the vulnerability tests, while paragraph 0149 describes daily alerts of newly detected vulnerabilities. Paragraph 0054 describes a customer profile 204 (e.g., IP addresses and services to be provided) that may be used to conduct appropriate tests of the customer system. However, this is not a security policy of an enterprise which owns or controls said network Lastly, paragraph 0019 discloses updating the vulnerability library (of vulnerability tests that may be performed), and makes no mention of a security policy of an enterprise which owns or controls said network. Therefore, Bunker does not disclose *each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network,* as recited in claim 6.

Accordingly, Appellants respectfully request that the rejection of claim 6 be reversed, and the application returned to the examining group for allowance.

Claim 12

The rejection of claim 12 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 12 depends from allowable independent claim 1, and additionally recites *the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points*. The Examiner contends that Bunker discloses these features at paragraph 0073 (Final Office Action, page 18). Appellants respectfully disagree.

The passage identified by the Examiner is totally silent as to categorizing devices that transfer data across the perimeter of the network, much less as to categorizing such devices as control points or non-control points. Instead, at paragraph 0073, Bunker describes determining which basic tests 516 to run, and assigning the tests 516 to a Tester 502. Bunker simply does not disclose categorizing devices as control points or non-control points in this, or any other, passage.

Accordingly, Appellants respectfully request that the rejection of claim 12 be reversed, and the application returned to the examining group for allowance.

Claim 13

The rejection of claim 13 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 13 depends indirectly from allowable independent claim 1, and additionally recites *the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans; and testing control points with penetration tests*. The Examiner asserts that Bunker discloses

these features at paragraphs 0094-0095 (Final Office Action, page 18). Appellants respectfully disagree.

Appellants acknowledge that Bunker discloses port scans at paragraph 0095. However, as discussed *supra* with respect to claim 12 (from which claim 13 depends), Bunker does not disclose categorizing devices as either control points or non-control points. As such, Bunker cannot reasonably be said to disclose *testing control points with port scans; and testing control points with penetration tests,* as recited in claim 13. Put another way, there is no disclosure that Bunker's port scan is used to test an element previously categorized as a control point. Moreover, Bunker is completely silent as to penetration tests.

Accordingly, Appellants respectfully request that the rejection of claim 13 be reversed, and the application returned to the examining group for allowance.

Claim 14

The rejection of claim 14 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 14 depends from allowable independent claim 1, and additionally recites:

> performing a policy review of an enterprise which owns or controls said network;
> defining review parameters based upon the policy review; and
> utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

The Examiner asserts that Bunker discloses these features at paragraphs 0010-0012, 0059, 0149, and 0054 (Final Office Action, page 18-20). Appellants respectfully disagree.

The passages referred to by the Examiner describe the multi-part vulnerability test. However, these passages do not disclose utilizing parameters determined in a policy review in each of (i) a network perimeter architecture review, (ii) a device review, or (iii) an applications review. That is, Bunker does not disclose performing a first review (e.g., a policy review), defining parameters based upon the first review, and then using the defined parameters to perform four other types of reviews (e.g., (i) a network perimeter architecture review, (ii) a device review, (iii) an applications review, and (iv) a vulnerability review).

Accordingly, Appellants respectfully request that the rejection of claim 14 be reversed, and the application returned to the examining group for allowance.

Claim 15

The rejection of claim 15 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 15 depends from allowable independent claim 1, and additionally recites:

> the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases;
> the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases;
> the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and
> the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases.

The Examiner asserts that Bunker discloses these features at paragraphs 0010-0012, 0054, 0069-0083, and 0095 (Final Office Action, page 20). Appellants respectfully disagree.

As already discussed herein, Bunker does not disclose an architecture review or a policy review, much less that *the reviewing security of a network perimeter architecture comprises*

receiving review parameters from a policy review and generating test cases. Moreover, as Bunker does not disclose a policy review, Bunker cannot arguably disclose *the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters [from the policy review], receiving the test cases, and performing the test cases.* Similarly, since Bunker does not disclose review parameters associated with a policy review, Bunker cannot reasonably be said to disclose: *the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases*; or, *the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases.*

Accordingly, Appellants respectfully request that the rejection of claim 15 be reversed, and the application returned to the examining group for allowance.

Claims 16 and 17

Independent Claim 16

The rejection of independent claim 16 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Independent claim 16 recites:

> 16. A computer program product comprising a computer usable medium having a computer readable program embodied in the medium, wherein the computer readable program when executed on a computing device is operable to cause the computing device to:
> review security of a network perimeter architecture;
> review security of data processing devices that transfer data across the perimeter of the network;
> review security of applications that transfer data across said perimeter;

review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generate a report concerning security of said perimeter based upon all said reviews.

The Examiner asserts that "the computer program product and system claims are one of the same therefore rejected for the same reason as the method claims 1-15 above" (Final Office Action, page 21). Appellants respectfully disagree.

Appellants initially submit that the Examiner has failed to properly establish a *prima facie* case of anticipation with respect to claim 16 because the rejection does not address all of the features recited in claim 16. More specifically, Appellants submit that claim 16 recites features that are not recited in any of claims 1-15 (e.g., a computer program product comprising a computer usable medium having a computer readable program embodied in the medium), such that merely grouping claim 16 with the rejection of claims 1-15 cannot serve to establish a *prima facie* case of anticipation with respect to claim 16.

This makes the rejection fatally defective on its face, since MPEP §2143.03 states: "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Moreover, 37 C.F.R. §1.104 states: "[t]he examination shall be complete with respect both to compliance of the application or patent under reexamination with the applicable statutes and rules and to the patentability of the invention as claimed ..." (emphasis added). Moreover, MPEP §707.07(d), states that "[a] plurality of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group." In this case, the Examiner has improperly grouped claim 16 with the rejection of other claims while failing to address the language of claim 16.

In any event, Appellants submit that Bunker does not disclose all of the features recited in claim 16. Appellants incorporate the arguments discussed above with respect to claim 1. According to those arguments, Appellants submit that Bunker does not disclose reviewing security of a network perimeter architecture, reviewing security of data processing devices that transfer data across the perimeter of the network, reviewing security of applications that transfer data across said perimeter, and reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Further according to those arguments, Appellants submit that Bunker does not disclose generating a report concerning security of said perimeter based upon all said reviews.

Moreover, Appellants submit Bunker does not disclose *a computer program product comprising a computer usable medium having a computer readable program embodied in the medium* and arranged to perform the four recited reviewing and generating steps. Appellants acknowledge that Bunker discloses a computer program product. However, Appellants submit that Bunker does not disclose a computer program product that causes a computer to perform the recited functions. Therefore, Bunker does not disclose all of the features of claim 16.

For all of the above-noted reasons, Appellants submit that the rejection of claim 16 is improper. Accordingly, Appellants respectfully request the Board reverse the Examiner's decision to reject claim 16 and return the application to the examining group for allowance.

Claim 17

The rejection of claim 17 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 17 depends from allowable independent claim 16, and additionally recites

> ... each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the

> perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

The Examiner asserts that claims 16-20 are rejected for the same reasons as claims 1-15 (Final Office Action, page 21). Appellants respectfully disagree.

Appellants initially argue that the Examiner has failed to establish a *prima facie* case of anticipation with respect to claim 17 because the explanation of the rejection does not address all of the features recited in the claim. More specifically, claim 17 recites that each of the reviewing steps *utilize review parameters defined in a policy review of an enterprise which owns or controls said network.* This recitation is not present in claims 1-15. Therefore, the rejection of claims 1-15 is insufficient to establish a *prima facie* case of anticipation with respect to claim 17. Put another way, in light of MPEP §2143.03, 37 C.F.R. §1.104, and MPEP §707.07(d), Appellants submit that the Examiner has improperly grouped claim 17 with the rejection of other claims while failing to address the language of claim 17.

In any event, Appellants submit that Bunker does not disclose the invention recited in claim 17. Claim 17 recite that each of the four reviewing steps *utilize review parameters defined in a policy review of an enterprise which owns or controls said network.* As discussed above with respect to claim 14, Bunker does not disclose performing a first review (e.g., a policy review) to define parameters, then utilizing those parameters in four other types of reviews (e.g., (i) a network perimeter architecture review, (ii) a device review, (iii) an applications review, and (iv) a vulnerability review). Instead, Bunker only discloses a multi-wave vulnerability attack, wherein each wave is adjusted based upon data determined in the previous wave. However, such a vulnerability attack simply does not address the other types of review: (i) a network perimeter

architecture review, (ii) a device review, or (iii) an applications review. Therefore, Bunker cannot be said to disclose that each of the four reviews *utilize review parameters defined in a policy review of an enterprise which owns or controls said network*, as recited in claim 17.

Accordingly, Appellants respectfully request that the rejection of claim 17 be reversed, and the application returned to the examining group for allowance.

Claims 18-20

Independent Claim 18 and Dependent claim 19

The rejection of independent claim 18 and dependent claim 19 under 35 U.S.C. §102(b) is in error, and the decision to reject these claims should be reversed.

Independent claim 18 recites:

> 18. A system, comprising:
> a network having a perimeter; and
> a terminal connected to the network and arranged to:
> review security of a network perimeter architecture;
> review security of data processing devices that transfer data across the perimeter of the network;
> review security of applications that transfer data across said perimeter;
> review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and
> generate a report concerning security of said perimeter based upon all said reviews.

The Examiner asserts that "the computer program product and system claims are one of the same therefore rejected for the same reason as the method claims 1-15 above" (Final Office Action, page 21). Appellants respectfully disagree.

Appellants initially submit that the Examiner has failed to properly establish a *prima facie* case of anticipation with respect to claim 18 because the rejection does not address all of

the features recited in claim 18. More specifically, Appellants submit that claim 18 recites features that are not recited in any of claims 1-15 (e.g., a network and a terminal connected to the network), such that merely grouping claim 18 with the rejection of claims 1-15 cannot serve to establish a *prima facie* case of anticipation with respect to claim 18.

As discussed above with respect to claim 16, this makes the rejection unsustainable, since MPEP §2143.03 states: "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Moreover, 37 C.F.R. §1.104 states: "[t]he examination shall be complete with respect both to compliance of the application or patent under reexamination with the applicable statutes and rules and to the patentability of the invention as claimed …" (emphasis added). Moreover, MPEP §707.07(d), states that "[a] plurality of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group." In this case, the Examiner has improperly grouped claim 18 with the rejection of other claims while failing to address the language of claim 18.

In any event, Appellants submit that Bunker does not disclose all of the features recited in claim 18. Appellants incorporate the arguments discussed above with respect to claim 1. According to those arguments, Appellants submit that Bunker does not disclose reviewing security of a network perimeter architecture, reviewing security of data processing devices that transfer data across the perimeter of the network, reviewing security of applications that transfer data across said perimeter, and reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Further according to those arguments, Appellants submit that Bunker does not disclose generating a report concerning security of said perimeter based upon all said reviews.

Moreover, Appellants submit that Bunker does not disclose *a terminal connected to the network having a perimeter* and arranged to perform the four recited reviewing and generating steps. That is to say, not only does Bunker fail to disclose the reviewing and generating, but Bunker also fails to disclose that a terminal is arranged to perform the reviewing and generating. Instead, Bunker discloses plural testers 502 that launch a security tests (paragraph 0094). Bunker does not disclose that any one of the testers 502 is arranged to: review security of a network perimeter architecture; review security of data processing devices that transfer data across the perimeter of the network; review security of applications that transfer data across said perimeter; review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and generate a report concerning security of said perimeter based upon all said reviews. Therefore, Bunker does not recite a terminal connected to the network having a perimeter where the terminal is arranged to perform the functions recited in claim 18.

For all of the above-noted reasons, Appellants submit that the rejection of claim 18 is improper. Moreover, as claim 19 depends from claim 18, the rejection of claim 19 is improper for at least the same reasons. Accordingly, Appellants respectfully request the Board reverse the Examiner's decision to reject claims 18 and 19 and return the application to the examining group for allowance.

Claim 20

The rejection of claim 20 under 35 U.S.C. §102(b) is in error, and the decision to reject this claim should be reversed.

Claim 20 depends from allowable independent claim 18, and additionally recites:

> ... each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the

> perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

The Examiner asserts that claims 16-20 are rejected for the same reasons as claims 1-15 (Final Office Action, page 21). Appellants respectfully disagree.

Appellants initially argue that the Examiner has failed to establish a *prima facie* case of anticipation with respect to claim 20 because the explanation of the rejection does not address all of the features recited in the claim. More specifically, claim 20 recites that each of the reviewing steps *utilize review parameters defined in a policy review of an enterprise which owns or controls said network.* This recitation is not present in claims 1-15. Therefore, the rejection of claims 1-15 is insufficient to establish a *prima facie* case of anticipation with respect to claim 20. In light of MPEP §2143.03, 37 C.F.R. §1.104, and MPEP §707.07(d), Appellants submit that the Examiner has improperly grouped claim 20 with the rejection of other claims while failing to address the language of claim 20.

In any event, Appellants submit that Bunker does not disclose the invention recited in claim 20. Claim 20 recites that each of the four reviews *utilize review parameters defined in a policy review of an enterprise which owns or controls said network.* As discussed above with respect to claims 14 and 17, Bunker does not disclose performing a policy review to define parameters, then utilizing those defined parameters in four other types of reviews (e.g., (i) a network perimeter architecture review, (ii) a device review, (iii) an applications review, and (iv) a vulnerability review). Instead, Bunker only discloses a multi-wave vulnerability attack, wherein each wave is adjusted based upon data determined in the previous wave. However, such a vulnerability attack simply does not address the other types of review: (i) a network perimeter

architecture review, (ii) a device review, or (iii) an applications review. Therefore, Bunker cannot be said to disclose that each of the four reviews *utilize review parameters defined in a policy review of an enterprise which owns or controls said network*, as recited in claim 20.

Accordingly, Appellants respectfully request that the rejection of claim 20 be reversed, and the application returned to the examining group for allowance.

Conclusion

In view of the foregoing remarks, Appellants submit that claims 1-20 are patentably distinct from the prior art of record and are in condition for allowance. Accordingly, Appellants respectfully request that the Board reverse the Examiner's rejection of claims 1-20 and remand the application to the Examiner for allowance of the pending claims.

Respectfully submitted,
W. Carey BUNN et al.

Andrew M. Calderon
Registration No. 38,093

February 19, 2008
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

(VIII) CLAIMS APPENDIX

The following is a listing of the claims involved in the appeal.

1. A method for checking network perimeter security, said method comprising the steps of:

reviewing security of a network perimeter architecture;

reviewing security of data processing devices that transfer data across the perimeter of the network;

reviewing security of applications that transfer data across said perimeter;

reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generating a report concerning security of said perimeter based upon all of the reviewing steps.

2. The method as set forth in claim 1 further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter.

3. The method as set forth in claim 1 further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter.

4. The method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server.

5. The method as set forth in claim 1 further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network.

6. The method as set forth in claim 1 wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network.

7. The method as set forth in claim 1 further comprising the step of determining said network perimeter.

8. The method as set forth in claim 7 wherein said network perimeter comprises entries and exits from said network.

9. The method as set forth in claim 1 wherein said network perimeter comprises entries and exits from said network.

10. The method as set forth in claim 1 wherein the steps of reviewing security of a network perimeter architecture, reviewing security of data processing devices that transfer data across the perimeter of the network, and reviewing vulnerability of applications or data

processing devices within said perimeter from entities outside of said perimeter are performed at least in part with a respective program tool.

11. The method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter.

12. The method as set forth in claim 1, wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points.

13. The method as set forth in claim 12, wherein the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises:

testing control points with port scans; and

testing control points with penetration tests.

14. The method as set forth in claim 1, further comprising:

performing a policy review of an enterprise which owns or controls said network;

defining review parameters based upon the policy review; and

utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said

perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

15. The method as set forth in claim 1, wherein:

the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases;

the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases;

the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and

the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases.

16. A computer program product comprising a computer usable medium having a computer readable program embodied in the medium, wherein the computer readable program when executed on a computing device is operable to cause the computing device to:

review security of a network perimeter architecture;

review security of data processing devices that transfer data across the perimeter of the network;

review security of applications that transfer data across said perimeter;

review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generate a report concerning security of said perimeter based upon all said reviews.

17. The computer program product of claim 16, wherein each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

18. A system, comprising:

a network having a perimeter; and

a terminal connected to the network and arranged to:

review security of a network perimeter architecture;

review security of data processing devices that transfer data across the perimeter of the network;

review security of applications that transfer data across said perimeter;

review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generate a report concerning security of said perimeter based upon all said reviews.

19. The system of claim 18, wherein the report is based upon data provided by the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter

20. The system of claim 18, wherein each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

(IX) EVIDENCE APPENDIX

NONE.

(X) RELATED PROCEEDINGS APPENDIX

NONE.